Coordinating Agency:

Department of Homeland Security/National Protection and Programs/Cyber Security and Communications/National Cyber Security Division

Cooperating Agencies:

Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation
Department of the Treasury
Office of the Director of National Intelligence
National Institute of Standards and Technology
Office of Management and Budget

INTRODUCTION

Purpose

The purpose of the Cyber Incident Annex is to outline the policies, organization, actions, and responsibilities for a coordinated, broad-based approach to incidents requiring coordinated Federal response that are induced by cyber means or have cyber effects. A physical attack on cyber infrastructure is covered by ESF #2 – Communications.

Scope

This annex describes the framework for Federal Cyber Incident response coordination among Federal departments, agencies, and upon request, State, local, tribal, and private-sector entities. The Cyber Incident Annex is built primarily upon the National Strategy to Secure Cyberspace, Homeland Security Presidential Directive 7 (HSPD-7), and the National Infrastructure Protection Plan (NIPP). The national cyberspace response system is a public-private architecture that provides mechanisms for rapid identification, information exchange, response, and remediation in order to mitigate the damage caused by malicious cyberspace activity.

This annex focuses on responding to and recovering from cyber incidents requiring a coordinated Federal response (hereafter referred to as a "Cyber Incident") that impact mission-critical functions and/or threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation. A cyber incident is induced directly through cyber means with cyber or physical results that:

- Cause, or are likely to cause, harm to mission-critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or

- Threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation.

Such an incident would likely affect communications and/or computing services in at least one and possibly several metropolitan areas and/or States. It would involve multiple communications service providers and/or IT products and applications, resulting in a significant degradation of the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of communication and computing services for at least a significant portion of a business day or longer.

This annex describes the specialized application of the National Response Framework to a Cyber Incident. When a Cyber Incident occurs it could impact multiple infrastructure sectors or be targeted at a specific sector such as finance, energy, or communications. A Cyber Incident may result in the activation of all Emergency Support Function (ESF) Annexes under the National Response Framework, as appropriate. The National Communications System (NCS), as the primary agency for ESF #2, works closely with the Department of Homeland Security/National Cyber Security Division (DHS/NCSD) to coordinate ESF #2 during Cyber Incidents.

Policies

This annex:

- Supports the mission and construct of the Office of Cybersecurity and Communications (CS&C).
- Involves the private sector as described in HSPD-7.
- Refers to the National Response Framework's International Coordination Support Annex for international support activities relating to a Cyber Incident.
- Refers to the National Response Framework's Critical Infrastructure/Key Resources (CI/KR) Support Annex for coordination across multiple CI/KR sectors.
- Is implemented within the structure and operating principles of the National Response Framework and pursuant to the following authorities:
  - The enhancement of Non-Federal Cyber Security, the Homeland Security Act (Section 223, Public Law 107-276)
  - HSPD-5: Management of Domestic Incidents
  - HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection
  - The Federal Information Security Management Act (FISMA)
  - Executive Order 12472: The Assignment of National Security Emergency Preparedness Responsibilities for Telecommunications
  - Section 706, the Communications Act of 1934, as amended (47 U.S.C. 606)
  - The Defense Production Act of 1950, as amended
  - The National Security Act of 1947, as amended
  - National Security Directive 42: National Policy for the Security of National Security Telecommunications and Information Systems
  - The National Strategy To Secure Cyberspace
  - The NIPP
  - Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458, 118 Stat. 3638)
  - Intelligence Authorization Act for Fiscal Year 2004 (Public Act 108-177)

CONCEPT OF OPERATIONS

General

A Cyber Incident may overwhelm government and/or private-sector resources by disrupting the Internet and/or taxing critical infrastructure information systems. Complications from a Cyber Incident may threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the nation. Rapid identification, information exchange, investigation, and coordinated response and remediation often can mitigate the damage that could be caused by this type of incident.

As the focal point for the public and private sectors regarding cyber security issues[1], DHS/NCSD is responsible for the public-private coordination in response to a Cyber Incident, which includes:

- Coordinating national-level cyber response and recovery efforts.
- Providing alerts and notification of potential cyber threats, incidents, and attacks.
- Sharing information both inside the government and with the private sector, including best practices, incident response, and incident mitigation.
- Analyzing cyber vulnerabilities, exploits, and attack methods.
- Providing technical assistance.
- Defending against the attack.

These activities are the product of, and require, a concerted effort by Federal, State, tribal, and local governments, as well as nongovernmental entities, such as the private sector and academia. In order to support the objectives of this annex, ESF #2 may be activated to assist in providing an operational response structure, fiduciary mechanisms, and reporting capabilities to effectively respond to a Cyber Incident.

Additionally, it is essential that the Federal Government coordinate closely with the appropriate entities to ensure the most effective response to a Cyber Incident. DHS/NCSD's Private Sector Concept of Operations (ConOps) identifies the mechanisms necessary for coordinating actions between private-sector partners and the NCSD, United States Computer Emergency Readiness Team (US-CERT), and National Cyber Response Coordination Group (NCRCG) during a Cyber Incident.

ORGANIZATION

The following organizations play a role in responding to Cyber Incidents:

- **National Cyber Security Division (NCSD):** The NCSD is part of the Office of CS&C and serves as the national focal point for working collaboratively with public, private, and international entities regarding cyber security issues[2]. DHS/NCSD has two overarching objectives: (1) to build and maintain an effective national cyber response system, and (2) to implement a cyber risk management program for the protection of critical infrastructure. DHS/NCSD is responsible for identifying, analyzing, and reducing cyber risks and

[1] "Cyber security issues" refers to the technical aspects of cyber security, to include alert and warning. The Department of Justice is the focal point for law enforcement's response to cyber security issues.
[2] See footnote 1.

vulnerabilities; disseminating threat warning information; coordinating incident response; and providing technical assistance in continuity of operations and recovery planning. DHS/NCSD will support the Department of Justice (DOJ) and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.

- **The United States Computer Emergency Readiness Team (US-CERT):** US-CERT, an operational component of DHS/NCSD, coordinates pertinent warnings among Federal departments and agencies. US-CERT also maintains a 24/7 operations center with connectivity to all major Federal cyber operations centers and private-sector Internet service providers, information-sharing mechanisms, and vendors. In addition, US-CERT, in concert with the National Operations Center (NOC), acts as a nexus for collecting and disseminating information received from public and private-sector sources to the appropriate audiences. Through the duration of a Cyber Incident, US-CERT provides technical and operational support to the NCRCG, and interacts with the private and public sectors on a continual basis.

- **National Cyber Response Coordination Group (NCRCG):** The NCRCG is the principal interagency body in which Federal organizations responsible for a wide range of activities, including technical response and short-term recovery, law enforcement, intelligence, and defensive measures, coordinate for the purposes of executing an efficient and effective response to cyber incidents and threats. In the event of a Cyber Incident, the NCRCG is convened to harmonize operational efforts and facilitate information sharing.

  The NCRCG performs the following functions:

  - Provides input to member agency and department heads and the NOC on cyber security issues, incidents, and threats.
  - Provides strategic situational awareness and decisionmaking support pertaining to Cyber Incidents.
  - Coordinates recommendations for key interagency leadership to include the DRG, and other appropriate officials.
  - Facilitates interagency decisionmaking pertaining to the response, including the allocation of Federal cyber-related resources.
  - Supports the Executive Office of the President, as necessary.

  During an actual or potential Cyber Incident, the NCRCG coordinates with the NOC in disseminating critical information to and from government and nongovernment sources, including the private-sector partners, academia, and the general public. The NCRCG leverages existing resources of US-CERT in this coordination and outreach activity. DHS/NCSD serves as the Executive Agent for the NCRCG.

- **Incident Management Planning Team (IMPT):** The IMPT, as part of the NOC planning element, supports the development of strategic guidance, concepts and plan development, and plan refinement leading to the publication of a series of plans for actual or potential domestic incidents.

- **Domestic Readiness Group (DRG):** In the event other interagency organizations, such as the IMPT and/or the NCRCG, are unable to reach a consensus on a recommendation/decision, the DRG is convened to finalize the recommendation/decision.

- **Office of the Director of National Intelligence (ODNI):** The ODNI operates the Intelligence Community – Incident Response Center (IC-IRC), a 24/7 operation that facilitates the sharing of cyber event information among IC members in order to protect the IC's ability to collect, analyze, and disseminate intelligence via its networks. The IC-IRC is the single focal point for requesting assistance from the IC in conjunction with a Cyber Incident, and as such is responsible for coordinating with other incident response organizations including US-CERT and the NOC, in order to best leverage the authorities and capabilities of the IC in responding to Cyber Incidents.

- **Department of Defense (DOD):** DOD entities responsible for computer security and computer network defense may exercise those duties in support of the national response effort in four primary roles: 1) Defense Support of Civil Authorities; 2) intelligence and information sharing; 3) law enforcement investigations; and 4) military operations to defend the homeland. DOD capabilities include Intelligence components (the National Security Agency (NSA), the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Organization, and military intelligence components), Defense criminal investigative organizations (law enforcement and counterintelligence), Network Operation Security Centers, and Computer Emergency Response Teams. These entities, in cooperation with other Federal entities, as appropriate, provide attack sensing and warning capabilities, gather and analyze information to characterize the attack and to gain attribution of the cyber threat, participate in information sharing, offer mitigation techniques, perform network intrusion diagnosis, and provide technical expertise. DOD capabilities also include military operational units, which defend the DOD global information grid. DOD can take action to deter or defend against cyber attacks which pose an imminent threat to national security, as authorized by applicable law and policy. The NSA/Central Security Service Threat Operations Center (NTOC) Ops Floor enhances NSA's ability to help defend the Nation's critical networks by providing the means for synchronization across multiple organizations involved with detecting and responding to cyber threats. The floor provides a collaborative space for members of the IC, DOD, law enforcement, and DHS to coordinate, control, and focus sensors and activities across networks of interest. Additionally, it offers an environment where all organizations can fuse information and analytic results to characterize, attribute, deconflict, and respond to cyber threats and attacks.

- **Department of Justice/Federal Bureau of Investigation (DOJ/FBI):** DOJ/FBI, working with other law enforcement agencies, lead the national effort to investigate and prosecute cybercrime. The Attorney General has lead responsibility for criminal investigations of terrorist acts or terrorist threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad, where such acts are within the Federal criminal jurisdiction of the United States. DOJ, in cooperation with other Federal departments and agencies engaged in activities to protect national security, also coordinates the activities of the other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States. DOJ, working with other law enforcement agencies and the intelligence community, uses its authorities to attribute the source of a cyber attack. Among other things, DOJ works with the private sector in regard to the prevention, investigation, and prosecution of cybercrime. DOJ coordinates with DHS to provide domestic investigative information relevant to DHS analysis of the vulnerability of the cyber infrastructure to terrorist attack or to DHS analysis of terrorist threats against the cyber infrastructure.

- **Department of Homeland Security/U.S. Secret Service (DHS/USSS):** DHS/USSS works with DOJ/FBI and other law enforcement agencies in helping to lead the national effort to investigate and prosecute cybercrime. DHS/USSS coordinates with DOJ to assist in providing domestic investigative information used in DHS analysis of the vulnerability of the cyber infrastructure to terrorist attacks.

- **Information Sharing and Analysis Centers (ISACs):** The sector-specific ISACs (i.e., Information Technology ISAC, Communications ISAC, Financial Services ISAC, etc.) are trusted communities of security specialists from companies within the various industries. The ISACs and their members identify, analyze, and share information, identify and collaborate on vulnerabilities, and share best practices to protect their respective industries from cyber and physical threats.

- **Joint Telecommunications Resource Board (JTRB):** The JTRB is an interagency coordination group chaired by the Office of Science and Technology Policy (OSTP) and staffed by senior Federal officials to assist in the exercise of assigned non-wartime emergency telecommunications functions. The JTRB may be convened for major disasters, major failures or disruptions, abnormal telecommunications patterns or congestion, known or suspected sabotage, service curtailment on Government networks, national level emergencies or at the direction of the Director. The JTRB resolves conflicts regarding National Security/Emergency Preparedness (NS/EP) communications priorities and resources that cannot be resolved at lower levels.

ACTIONS

Preincident

Federal departments and agencies maintain computer incident response capabilities for daily situational awareness that can rapidly respond to cyber incidents on their networks, including events of prolonged duration. The NCSD and US-CERT can assemble the resources provided by law enforcement, the IC, DOD, and private-sector entities (e.g., ISACs) that also maintain mechanisms to improve the Nation's readiness capabilities in addressing Cyber Incidents. For example, DOJ has a network of prosecutors trained in handling cyber crime. DOJ/Federal Bureau of Investigation (FBI) and DHS/U.S. Secret Service (USSS) also have agents that specialize in high-tech investigations. Law enforcement's international cyber crime network enables investigators to rapidly obtain electronic data and evidence from foreign countries.

Notification and Activation Procedures

The activities described in this section of the Cyber Incident Annex are implemented when a Cyber Incident is suspected, imminent, or already underway.

The NCRCG receives information about cyber threats through a variety of communications channels that exist between the Federal Government, nongovernmental entities, and the public. When it is believed that a Cyber Incident is suspected, imminent, or already underway, the NCRCG is convened and notifies the NOC and private-sector organizations, as appropriate.

The following communication channels are used for notification and activation:

- **The National Cyber Alert System:** This system provides an infrastructure, managed by US-CERT, for relaying timely and actionable computer security updates and warning information to all users.

- **National Operations Center:** This is the primary national-level hub for domestic incident management communications and operations.

- **DOD Global NetOps Center:** This is the primary DOD command center for directing operations and defense of the DOD Global Information Grid and coordinating with the US-CERT.

- **Homeland Security Information Network (HSIN) Critical Sector (CS):** This communications network provides States and critical infrastructure owners and operators with real-time interactive connectivity to the NOC on a Sensitive-but-Unclassified (SBU) level to all users. HSIN-CS is the NOC's primary suite of tools for information sharing, coordination, planning, mitigation, and response.

- **HSIN/US-CERT Portal:** This secure collaboration tool enables private and public sectors to actively share information about cyber security vulnerabilities, exploits, and incidents in a trusted and secure environment among members.

- **US-CERT Public Web Site:** www.uscert.gov provides the primary means for US-CERT to convey information to the public at large. The site includes relevant information on cyber security issues, cyber activity, and vulnerability resources.

- **Critical Infrastructure Warning Information Network (CWIN):** This network provides out-of-band (e.g., not dependent on the Internet or public switched network) connectivity to government and industry participants. The network is engineered to provide a reliable and survivable network capability.

- **ISACs:** Through secure websites and secure e-mail, information on infrastructure threats and vulnerabilities is provided to the members.

Initial Actions

US-CERT tracks potential cyber incidents and, depending on severity level (severity levels 3 through 5), reports them to the NCRCG. US-CERT notifies the NOC of cyber-related incidents. The NCRCG, in coordination with the IMPT/DRG, makes recommendations to the Secretary of Homeland Security.

US-CERT uses a standardized, repeatable, and reliable method to assess the criticality or severity of a new or emerging cyber security event. The initial step after gathering information is to assess its "severity" using a scale from 1 to 5. The Cyber Federal severity ratings are as follows:

Severity	Rating	Description
Minimal	1	Poses negligible impact on the Federal Government
Low	2	Poses very low impact on the Federal Government
Medium	3	Poses a potential impact on the Federal Government
High	4	Has impacted the Federal Government
Crisis	5	Has had a severe impact on the operational capacity of the Federal Government

In addition to the Cyber Federal severity ratings, US-CERT receives incident reports and assessments from the private sector to develop recommendations on cyber severity ratings.

When a Cyber Incident occurs, DHS/NCSD and NCS, through the NCRCG, coordinate with the Secretary of Homeland Security. In addition, DHS/NCSD provides subject-matter expertise and support to the JTRB when necessary.

In addition to participating in the NCRCG, some government agencies work individually under their own authorities to fulfill their Cyber Incident response missions. Particularly, law enforcement and the IC work to identify and deter those responsible for Cyber Incidents and attacks.

DHS coordinates technical and other assistance with other Federal agencies and, upon request, for the State, tribal, and local governments and the private sector in response to a Cyber Incident.

Challenges and Considerations

The response to and recovery from a Cyber Incident must take into account existing challenges to the management of cyber incidents. In addition, entities involved in response and recovery efforts must consider the resulting effects that cyber and physical events have on one another. Such consideration allows resources to be appropriately channeled into resolving the identified challenges. Identifiable challenges include:

- **Management of Multiple Cyber Events:** The occurrence or threat of multiple Cyber Incidents may significantly hamper the ability of responders to manage these Cyber Incidents simultaneously. Strategic planning and exercises should be conducted to assist in addressing this problem and to identify potential solutions.

- **Availability and Security of Communications:** A debilitating infrastructure attack could impede communications needed for coordinating response and recovery efforts. A secure, reliable communications system is needed to enable public- and private-sector entities to coordinate efforts in the event that routine communications channels are inoperable.

- **Availability of Expertise and Surge Capacity:** Federal agencies must ensure that sufficient technical expertise is developed and maintained within the Government to address the wide range of ongoing cyber attacks and vulnerabilities. In addition, the ability to surge technical and analytical capabilities in response to Cyber Incidents that may occur over a prolonged period must be planned for, exercised, and maintained.